Patent
Attorney's Docket No. 040020-149

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

REQUEST FOR FILING CONTINUATION/DIVISIONAL APPLICATION UNDER 37 C.F.R. § 1.53(b)

Box PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

This is a request for filing a [ ] continuation [X] divisional application under 37 C.F.R. § 1.53(b) of pending Application No. 08/765,269 filed on February 18, 1997, for METHOD FOR ENCRYPTION OF INFORMATION, by the following named inventor(s):

(a) Full Name Roland BODIN

[X] The entire disclosure of the prior application from which a copy of the oath or declaration is supplied herewith is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

1. [X] Enclosed is a copy of the prior Application No. 08/765,269 as originally filed on February 18, 1997, including copies of the specification, claims, drawings and the executed oath or declaration as filed.

2. [ ] Enclosed is a revised prior application and a copy of the prior executed oath or declaration as filed. No new matter has been added to the revised application.

3. [ ] _____ statement(s) claiming small entity status [ ] are enclosed [ ] were filed in prior Application No. __, filed on __.

4. [X] The filing fee is calculated below [X] and in accordance with the enclosed preliminary amendment:

CLAIMS					
	NO. OF CLAIMS		EXTRA CLAIMS	RATE	FEE
Basic Application Fee					$760.00
Total Claims	1	MINUS 20 =	0	x $18.00 =	0.00
Independent Claims	1	MINUS 3 =	0	x $78.00 =	0.00
Total Application Fee					760.00
Add Assignment Recording Fee of $40.00 if Assignment document is enclosed					
TOTAL APPLICATION FEE DUE					**760.00**

5. [ ] Charge $ _____ to Deposit Account No. 02-4800 for the fee due.

6. [X] A check in the amount of $ 760.00 is enclosed for the fee due.

7. [X] The Commissioner is hereby authorized to charge any appropriate fees under 37 C.F.R. §§ 1.16, 1.17 and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800. This paper is submitted in triplicate.

8. [X] Cancel in this application original claims 1-4 of the prior application before calculating the filing fee. (At least one original independent claim must be retained for filing purposes.)

9. [X] Amend the specification by inserting before the first line the sentence: --This application is a divisional of Application No. 08/765,269, filed February 18, 1997--.

10. [ ] Transfer the drawings from the pending prior application to this application and abandon said prior application as of the filing date accorded this application. A duplicate of this paper is enclosed for filing in the prior application file. (May only be used if signed by person authorized under 37 C.F.R. § 1.138 and before payment of issue fee.)

11. [X] New drawings are enclosed.

12. [X] Priority of Application No. 9503343-7 filed on September 27, 1995 in Sweden (country) is claimed under 35 U.S.C. § 119.
[X] The certified copy of the priority application
[X] was filed on December 20, 1996 in prior Application
No. PCT/SE96/01156, filed on September 18, 1996

13. [X] A preliminary amendment is enclosed.

14. [ ] Also enclosed _____.

15. [X] The power of attorney in the prior application is to Burns, Doane, Swecker & Mathis, L.L.P..

a. [X] The power appears in the original papers in the prior application.

b. [ ] Since the power does not appear in the original papers, a copy of the power in the prior application is enclosed.

c. [X] Recognize as Associate Agent/Attorney Tony M. Cole (Reg. No. 43,417) .

d. [X] Address all future communications to: (May only be completed by applicant, or attorney or agent of record.)

Ronald L. Grudziecki, Esq.
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, Virginia 22313-1404

October 1, 1999
Date

By: Tony M. Cole
Tony M. Cole
Registration No. 43,417

ADDRESS OF SIGNATOR:

BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

[ ] inventor(s)
[ ] assignee of complete interest
[ ] attorney or agent of record
[X] filed under 37 C.F.R. § 1.34(a)

Patent
Attorney's Docket No. 040020-149

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	)	
	)	
Roland BOLIN	)	Group Art Unit: 2766
	)	
Application No.: Divisional of Application No. 08/765,269	)	Examiner: H. Sayadian
	)	
Filed: October 1, 1999	)	
	)	
For: METHOD FOR ENCRYPTION OF INFORMATION(As Amended)	)	
	)	

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Before examination on the merits, please amend the application as follows:

IN THE TITLE:

Please delete the old title and replace with --Method for Encryption of Information--.

IN THE SPECIFICATION:

Page 1, line 28, replace "an" with -- As described in ETSI/GSM 03.20, an --

Page 1, line 29, replace the comma with a period and insert -- As further described,-- before "an algorithm A5".

Page 1, line 31, insert a comma after "form".

Page 1, line 32, insert a comma after "Ki" and insert a period after "Kc".

Page 1, lines 32-33, delete "from a random number variable, RAND."

Page 2, line 35, delete the second occurrence of "random".

Page 3, lines 2-3, delete "in respect of authorization checks".

Page 3, line 20, insert a comma after "illustrates" and after "schematically".

Page 3, line 32, insert -- Figures 5-8 illustrate the method steps of the various exemplary embodiments of the present invention --.

Page 4, line 32, replace comma with a period, delete "although only", replace first "the" with --The--.

Page 5, line 21, replace "A5" with --A3--.

Page 8, line 3, after "PSm'" insert -- (see steps of Figure 7)--

Page 8, line 11, insert -- (see steps of Figure 5) -- before "or".

Page 8, line 15, insert --(see steps of Figure 6)-- before "used".

Page 8, line 23, insert -- (see steps of Figure 8)-- after "F_N".

Please append the abstract, enclosed on a separate sheet, to the specification.

IN THE CLAIMS:

Please cancel claims 1-4 without prejudice or disclaimer.

Please amend claim 5 as follows:

5. (Amended) A method of encrypting information transmitted between a fixed network [(N)] and a mobile station [(MS)] in a time division multiple access (TDMA) mobile radio system [that operates in accordance with the time division multiple access concept], wherein [the] information is divided into at least two blocks [(B1, B2)] and transmitted in at least two time slots [(TS1, TS2) corresponding to said blocks] in each frame in a frame sequence, [and wherein encryption is effected by] said method of encrypting information comprising the steps of:

a) forming a pseudo-random sequence [(PS)] from an encryption key [(Kc)] and an [the] ordinal number [(FN)] of the frame in which the information is transmitted in accordance with [a given] an encryption algorithm [(A5)];

[b) performing a logic operation (EXOR) between said pseudo-random sequence and each block of the non-encrypted information (INFO1);

characterized by]

[c)] b) forming a modified pseudo-random sequence [(PSm')] from said pseudo-random sequence, [(PS)] in dependence on the ordinal number [(TSn)] of the time slot within which the information block [(B1 or B2)] that is encrypted with the modified pseudo-random sequence shall be transmitted, in accordance with a [given] first algorithm [(ALG3)]; and

[d)] c) performing a [said] logic operation [(EXOR) on the] between said modified pseudo-random sequence [(PSm') for] and each block [(B1 and B2)] of [the] non-encrypted information.

REMARKS

Applicant notes that claim 5, as amended, corresponds to claim 10 of co-pending Application No. 08/765,269 (of which this application is a divisional). Claim 10 was not elected in response to a restriction requirement in the co-pending application. Furthermore, the amendments to the title and the specification correspond to amendments previously made in the co-pending application.

In view of the above amendments, further and favorable action in the form of a Notice of Allowance is earnestly solicited. If the Examiner has any questions concerning this Response, or the application in general, the Examiner is invited to contact the undersigned at the Examiner's earliest convenience.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

By: _____
Tony M. Cole
Registration No. 43,417

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

Date: October 1, 1999

ABSTRACT

The method involves modifying an encryption key (Kc) in accordance with a given algorithm and in dependence on the ordinal number of a time slot to obtain a modified encryption key. A modified pseudo-random sequence is formed from the resultant modified encryption key. The modification is carried out in accordance with the aid of an encryption algorithm. A logical operation is performed on the modified pseudo-random sequence and for each block of the non-encrypted information. Preferably the operation is performed on the information block that belongs to the time slot whose ordinal number has been used to form the modified encryption key. As an additional option, the frame number can also be modified in accordance with a given algorithm and in dependence on the ordinal number of the relevant time slot. The method provides reliable encryption in TDMA mobile radio systems in which two or more time slots are used for one and the same transmission without requiring any substantial changes to signaling protocol and/or system equipment.

AN INFORMATION ENCRYPTION METHOD

FIELD OF INVENTION

The present invention relates to a method of encrypting information between a stationary network and a mobile station in a mobile radio system of the time division multiple access type (TDMA system).

More specifically, the invention relates to methods of encrypting the transmitted information in a more secure fashion in conjunction with an authorization check on the mobile by the network and when a multiple of time slots are used for the same user (mobile station).

DESCRIPTION OF THE BACKGROUND ART

The GSM-network, common in Europe, is a mobile radio network that uses time division multiple access (TDMA). As with other mobile radio networks, the GSM network employs authorization checks and encryption of transmitted messages. With regard to the GSM network, this is specified in "GSM specification 03.20", May 1994, issued by ETSI (European Telecommunication Standard Institute) and hereinafter referred to as ETSI/GSM 03.20. The various algorithms used in authorization checks and encryption are described in this reference.

An algorithm A3 is used to effect actual authorization checks between network and subscriber apparatus, an algorithm A5 is used for encryption of the payload information to be transmitted, and an algorithm A8 is used to form from the subscriber authorization key Ki an encryption key Kc from a random number variable, RAND.

As a rule, only one time slot per frame for a given connection is used in TDMA-type time division mobile radio systems; see ETSI/GSM 05.02.

The use of two or more time slots, not necessarily consecutive time slots, in a transmission frame has been proposed, see ETSI/STC SMG3, T doc SMG3 WPA 95A dated 29th August 1995 (Nokia Telecommunications), see particularly point 5 "HSCSD Architecture". This provides the advantage of enabling larger quantities of information to be transmitted per unit of time (applicable particularly to data transmissions), but has the drawback of increasing bandwidth.

SUMMARY OF THE INVENTION

The inclusion in a GSM system of two or more time slots instead of one time slot for one and the same radio transmission in accordance with the aforegoing creates certain problems when encryption and authorization checks are to be employed.

The most obvious procedure would be to process each of the time slots separately and to process the information in accordance with earlier known principles. However, such procedures would require drastic modification to the existing signalling protocols and to equipment on both the network side and the mobile station side.

It would be desirable to avoid such modifications to existing standards and equipment to the greatest possible extent. The use of the same pseudo-random sequence for all time slots within one and the same frame and for a given frame number is proposed in the aforementioned ETSI document, ETSI/ T doc SMG3, "First HSCSD stage 2 draft". The drawback with this method is that it is necessary to compromise between encryption safety and procedure simplicity. When two separate bursts belonging to one and the same user are transmitted in this manner while using the same encryption sequence (pseudo-random random sequence), the influence of the encryption can be eliminated relatively simply, by carrying out simple EXOR operations.

The object of the present invention is therefore to provide methods for reliable encryption in respect of authorization checks in a TDMA-type mobile radio system in which two or more time slots are used for one and the same transmission without needing to make substantial changes to the signalling protocol and/or system equipment.

In this regard, an inventive method is characterized by the features set forth in the following Claim 1. Another inventive method is characterized by the features set forth in the accompanying Claim 3. Further inventive methods are characterized by the features set forth in accompanying Claims 4 and 5.

BRIEF DESCRIPTION OF THE DRAWINGS

The aforesaid inventive methods will now be described in more detail with reference to the accompanying drawings.

Figure 1 illustrates schematically signalling between a network side and a mobile station side in a mobile radio system during the authorization check procedure.

Figure 2 is a block diagram illustrating known information encryption in the system illustrated in Figure 1.

Figure 3 is a block diagram which symbolizes the algorithms used in two of the inventive methods.

Figure 4 is a block diagram symbolizing the algorithms used in a third inventive method.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Figure 1 is a simplified schematic illustration of a mobile radio system, for instance a GSM-system. The system has a network side "NETWORK" and a mobile station side "Mobile".

The network side includes a base station system BSS which is connected to a mobile switching centre MSC, which is connected, in turn, to the public telephone network (not shown). The base station system BSS typically includes a base transceiver station BTS and a base station controller BSC (not shown). In reality, a plurality of base station systems are connected to the mobile switching centre MSC on the network side, while the mobile station side includes a plurality of mobile stations that can communicate simultaneously with the base station system BSS. The network side and the mobile station side transmit information via radio signals over an air interface which is symbolized in Figure 1 with the reference TR.

Before the actual information is transmitted and received between the network and a given mobile station MS, the network is obliged to check the authorization of the mobile station MS. This authorization check is carried out in accordance with known principles, whereby the network, i.e. the base station system BSS, sends a random number (so-called "random challenge") RAND to the mobile station MS over a dedicated control channel DCCH.

The mobile station MS receives the random number RAND and forms a response SRES (signed response) from this random number and from the mobile station's own key Ki in accordance with a given algorithm A3, as described on page 50 of the aforesaid ETSI/GSM 03.20.

At the same time, the mobile station MS compiles an encryption key Kc from the key Ki in accordance with another algorithm A8, although only the response SRES is sent to the base station system BSS, while the encryption key Kc is used in the encryption carried out in the mobile station in accordance with the following. A comparison is made in the base station system BSS with corresponding values of SRES calculated by the mobile switching center (MSC) in accordance

with the same conventional algorithms A3 and A8 found in the mobile station MS. When a coincidental result is obtained, the mobile station is considered to be authorized and communication can continue. The continued information transmission will thereafter be encrypted in accordance with a given algorithm A5, as described on pages 48-49 of ETSI/GSM 03.20.

Thus, the network includes an algorithm block AN which stores and carries out an authorization check in accordance with the algorithms A3 and A8 and encryption in accordance with the algorithm A5. The mobile station MS includes a corresponding algorithm block AM which stores and carries out an authorization check in accordance with the same algorithms A3 and A8 and encryption in accordance with the algorithm A5.

The encryption key Kc is generated by the mobile switching center (MSC) on the basis of the mobile station's encryption key Ki, which is known to the mobile telephone switching centre. Subsequent to making the authorization check, (algorithm A5), the mobile telephone switching centre MSC sends the key Kc to the base station system BSS and encryption of payload information can be commenced with the aid of the agreed encryption key Kc.

Figure 2 illustrates schematically the manner in which the payload information is encrypted and formatted for transmission over two time slots TS1, TS2 in accordance with the aforesaid NOKIA proposal.

Normally, the payload information is divided from, e.g., a speech frame into one or more blocks each of 114 bits. One such block is encrypted in accordance with the algorithm A5 and sent during a burst in a given time slot, optionally interfoliated with another adjacent block. The next encrypted block then follows. As illustrated in Figure 2, when two time slots in a given frame are available, an information block

is now divided into two sub-blocks B1 and B2, each containing 114 bits, and each block is encrypted with the same pseudo-random sequence PS of 114 bits as normal, by carrying out two EXOR operations shown in Figure 2.

The pseudo-random sequence PS is obtained from an ordinal number FN of the frame in which the time slots TS1, TS2 are located whose information (blocks B1 and B2) shall be encrypted. Two encrypted information blocks BK1 and BK2 are obtained and these blocks are then formatted by inserting a sync. and training sequence in a known manner (marked with X in Figure 2). As before mentioned, the drawback with this encryption method is that the same encryption sequence is used two times for two separate time slots which means that non-encrypted information can be recovered from each of the two time slots by an EXOR operation between the encrypted information.

In accordance with the present invention, the time slot ordinal number or an equivalent to this number is inserted into the frame as a further parameter when encrypting. As a result, when transmitting in two time slots within the same frame, the transmitted information will be independently encrypted and encryption security therewith further enhanced in comparison to the case when only the frame number (in addition to the encryption key) is used. If, as is normal, a user uses only one time slot per frame, no time-slot dependent encryption is required because the user's authorization key is unique for a certain time slot. By modifying the input parameters (code key Kc, frame number FN) in direct dependence on the ordinal number of a time slot in a frame in accordance with the present invention, it is possible to apply the original algorithms without needing to make any substantial change to the signalling protocol, as before described, or to the radio equipment.

Figure 3 is a block diagram illustrating the use of the original algorithm A5 with modified input magnitudes in accordance with the present invention.

The block AB in Figure 3 symbolizes the original algorithm A5, which is specified in accordance with GSM 03.20. The encryption key Kc is now modified in accordance with the ordinal number TSn=TS1 of the relevant time slot, namely the time slot in the frame during which a first block B1 according to Figure 2 shall be transmitted (possibly interfoliated with an adjacent block, although the principle is the same). In this regard, circle 1 symbolizes a calculation algorithm ALG1 for obtaining a modified value Kc1 of the encryption key. The same algorithm can be used for all time slots in the frame, such that

$$ALG1(Kc,TSn) = Kcn'.$$

It is not necessary to modify all encryption keys and one key may be identical to the normal encryption key Kc for a given time slot.

Similarly, the frame ordinal number FN is modified in dependence on the ordinal number TSn=TS1 of the relevant time slot in the frame within which the first block B1 in Figure 2 shall be transmitted. Circle 2 therewith symbolizes a calculation algorithm ALG2 for obtaining the modified value FN' of the frame ordinal number. The same algorithm can be used for all time slots in the frame, such that

$$ALG2(FN,TSn) = FNn'.$$

The two algorithms ALG1 and ALG2 need not be equal.

Furthermore, one of the modified frame numbers FNn' may be identical to the normal FN.

In both of the aforesaid cases, there is obtained an output magnitude in the form of a modified pseudo-random sequence PSm' which is used in the same way as that shown in Figure 2.

It will be understood that the sequence PSm' can also be generated either

a) by solely using a modified value Kc' on the encryption key and an unchanged value FN on the frame number, i.e. the algorithm 2 is not used; or

b) by solely using a modified value FN' on the frame number FN and an unchanged value on the encryption key Kc, i.e. the algorithm 1 is not used.

Figure 4 is a block diagram similar to the block diagram of Figure 3, but now with totally unchanged input values Kc, FN to the algorithm A5. Instead, the time slot ordinal number TSn (or a value equivalent to said ordinal number) is used as a control value for an algorithm ALG3 symbolized by circle 3 for modifying the normal pseudo-random sequence PS obtained from Kc and FN. This algorithm ALG3 may consist in a certain permutation, shift, reordering of values, etc., in the pseudo-random sequence PS, so as to obtain a new sequence PSm'. The sequence may optionally be divided into blocks of 114 bits prior to reformulation, and the values in one or more blocks can be mixed to obtain the new values with an unchanged number of bits (114) in each block.

It is also possible to combine the algorithms ALG1,2 in Figure 3 with the algorithm ALG3 according to Figure 4.

The aforedescribed embodiments of the proposed method relate to transmission cases. It will be understood that in the case of reception wherein incoming information shall be decrypted, the values of Kc and FN and the sequence PS will be modified

to Kc', FN' and PSm' respectively in accordance with the agreed algorithms ALG1, ALG3 and ALG3 as described above.

CLAIMS

1. A method of encrypting information transmitted between a fixed network (MSC, BSS) and a mobile station (MS) in a mobile radio system that operates in accordance with the time division multiple access concept, wherein the information is divided into at least two blocks (B1, B2) and transmitted in at least two time slots (TS1, TS2) corresponding to said blocks in each frame in a frame sequence, and wherein encryption is effected by

a) forming a pseudo-random sequence (PS) in accordance with a given encryption algorithm (A5) from an encryption key (Kc) and the ordinal number (FN) of the frame in which the information is transmitted;

b) performing a logic operation (EXOR) between said pseudo-random sequence (PS) and each block (B1 and B2) of the non-encrypted information to obtain encrypted information (BK1, BK2);

characterized by

c) modifying said encryption key (Kc) in accordance with a given algorithm (ALG1) and in dependence on the ordinal number of a time slot (TSn) so as to obtain a modified encryption key (Kc');

d) forming a modified pseudo-random sequence (PSm') from the resultant modified encryption key (Kc') in accordance with aid encryption algorithm A5); and

e) performing said logic operation (EXOR) on the modified pseudo-random sequence (PSm') and for each block (B1 and B2) of the non-encrypted information.

2. A method according to Claim 1, **characterized** by carrying out the operation performed in accordance with e) on the information block (B1) that belongs to the time slot (TS1) whose ordinal number has been used to form said modified encryption key.

3. A method of encrypting information transmitted between a fixed network (N) and a mobile station (MS) in a mobile radio system that operates in accordance with the time division multiple access concept, wherein the information is divided into at least two blocks (B1, B2) and transmitted in at least two time slots (TS1, TS2) corresponding to said blocks in each frame in a frame sequence, and wherein encryption is effected by

a) forming a pseudo-random sequence (PS) in accordance with a given encryption algorithm (A5) from an encryption key (Kc) and the ordinal number (FN) of the frame in which the information is transmitted;

b) performing a logic operation (EXOR) between said pseudo-random sequence (PS) and each block (B1 and B2) of non-encrypted information to obtain encrypted information (BK1, BK2);

characterized by

c) modifying said frame number (FN) in accordance with a given algorithm (ALG2) and in dependence on the ordinal number of a relevant time slot (TSn);

d) forming a modified pseudo-random sequence (PSm') from the obtained modified frame number (FN') in accordance with said encryption algorithm (A5); and

e) performing said logic operation (EXOR) on the modified pseudo-random sequence (PSm') for each block (B1 and B2) of non-encrypted information.

4. A method of encrypting information transmitted between a fixed network (N) and a mobile station (MS) in a mobile radio system that operates in accordance with the time division multiple access concept, wherein the information is divided into at least two blocks (B1, B2) and transmitted in at least two time slots (TS1, TS2) corresponding to said blocks in each frame in a frame sequence, and wherein encryption is effected by

a) forming a pseudo-random sequence (PS) from an encryption key (Kc) and the ordinal number (FN) of the frame in which

the information is transmitted in accordance with a given encryption algorithm (A5);

b) performing a logic operation (EXOR) between said pseudo-random sequence and each block of the non-encrypted information (INFO1);

characterized by

c) modifying said encryption key (Kc) in accordance with a given algorithm (ALG1) and in dependence on the ordinal number of the relevant time slot (TSn);

d) forming a modified pseudo-random sequence (PSm') from the obtained modified encryption key (Kc') in accordance with said encryption algorithm (A5);

e) modifying said frame number (FN) in accordance with a given algorithm (ALG2) and in dependence on the ordinal number of a relevant time slot (TSn);

f) forming a modified pseudo-random sequence (PSm') from the obtained modified frame number (FN') in accordance with said encryption algorithm (A5); and

g) performing said logic operation (EXOR) on the modified pseudo-random sequence (PSm') for each block (B1 and B2) of the non-encrypted information.

5. A method of encrypting information transmitted between a fixed network (N) and a mobile station (MS) in a mobile radio system that operates in accordance with the time division multiple access concept, wherein the information is divided into at least two blocks (B1, B2) and transmitted in at least two time slots (TS1, TS2) corresponding to said blocks in each frame in a frame sequence, and wherein encryption is effected by

a) forming a pseudo-random sequence (PS) from an encryption key (Kc) and the ordinal number (FN) of the frame in which the information is transmitted in accordance with a given encryption algorithm (A5);

b) performing a logic operation (EXOR) between said pseudo-random sequence and each block of the non-encrypted information (INFO1);

characterized by

c) forming a modified pseudo-random sequence (PSm') from said pseudo-random sequence (PS) in dependence on the ordinal number (TSn) of the time slot within which the information block (B1 or B2) that is encrypted with the modified pseudo-random sequence shall be transmitted in accordance with a given algorithm (ALG3); and

d) performing said logic operation (EXOR) on the modified pseudo-random sequence (PSm') for each block (B1 and B2) of the non-encrypted information.

Patent
Attorney's Docket No. 040020-149

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	)	Attention: **Drafting Branch**
	)	
Roland BODIN	)	
	)	
Application No.: Divisional of Application No. 08/765,269	)	Group Art Unit: 2766
	)	Examiner: H. Sayadian
Filed: October 1, 1999	)	
	)	
For: METHOD FOR ENCRYPTION OF INFORMATION	)	

SUBMISSION OF FORMAL DRAWINGS

Box Issue Fee
Assistant Commissioner for Patents
Washington, D.C. 20231

ATTN: OFFICIAL DRAFTSMAN

Sir:

Enclosed please find four (4) sheet(s) of formal drawings for review by the Patent and Trademark Office in connection with the above-identified application. Please note that the drawings, which were submitted as Formal Drawings in parent Application No. 09/765,269 on September 27, 1999, include new Figs. 5-8 and label Figs. 1 and 2 "Prior Art". Should the enclosed drawings require changes, it is respectfully requested that the Patent and Trademark Office notify the undersigned agent of same.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

By: Tony M. Cole
Tony M. Cole
Registration No. 43,417

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

Date: October 1, 1999

Fig. 1
PRIOR ART

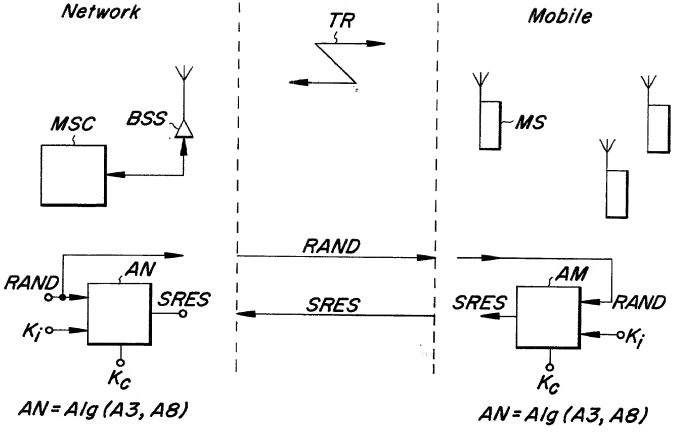


Fig. 2
PRIOR ART

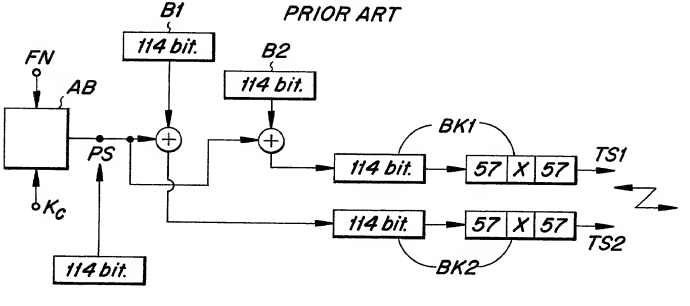
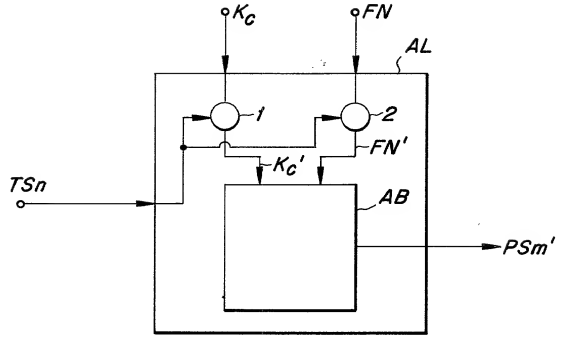


Fig. 3



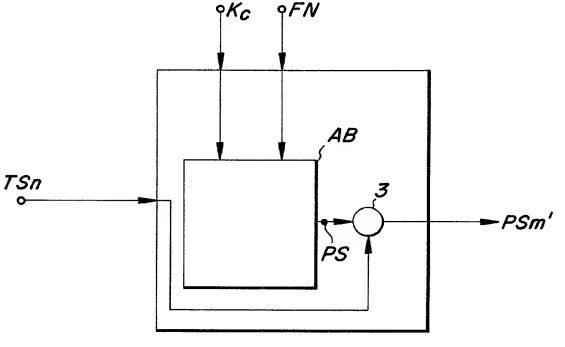


Fig. 4

Fig. 5

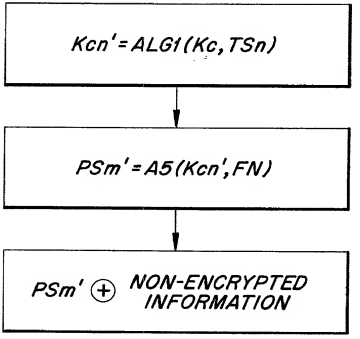

Kcn' = ALG1 (Kc, TSn)
PSm' = A5 (Kcn', FN)
PSm' ⊕ NON-ENCRYPTED INFORMATION

Fig. 6

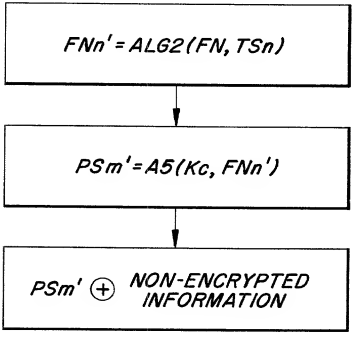

FNn' = ALG2 (FN, TSn)
PSm' = A5 (Kc, FNn')
PSm' ⊕ NON-ENCRYPTED INFORMATION

Fig. 7

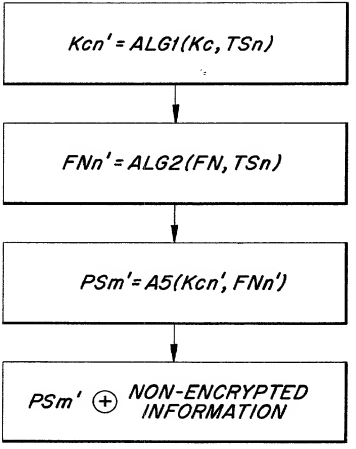
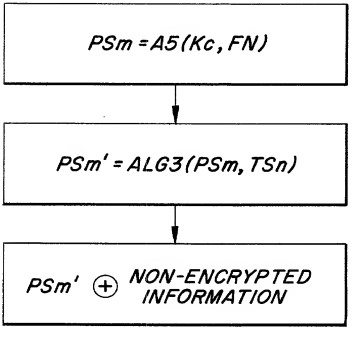

Kcn' = ALG1(Kc, TSn)
FNn' = ALG2(FN, TSn)
PSm' = A5(Kcn', FNn')
PSm' ⊕ NON-ENCRYPTED INFORMATION

Fig. 8


PSm = A5(Kc, FN)
PSm' = ALG3(PSm, TSn)
PSm' ⊕ NON-ENCRYPTED INFORMATION

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY (Includes Reference to Provisional and PCT International Applications)	ATTORNEY'S DOCKET NUMBER 027555-959

As a below named inventor, I hereby declare that:
My residence, post office address and citizenship are as stated below next to my name;
I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD FOR ENCRYPTION OF INFORMATION

the specification of which (check only one item below):

☐ is attached hereto.

☒ was filed as United States application

Number _____

on December 20, 1996

and was amended

on _____ (if applicable).

☐ was filed as PCT international application

Number _____

on _____

and was amended under PCT Article 19

on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 (a)-(e) of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

PRIOR FOREIGN/PCT APPLICATION(S) AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. §119:

COUNTRY (if PCT, indicate "PCT")	APPLICATION NUMBER	DATE OF FILING (day, month, year)	PRIORITY CLAIMED UNDER 35 U.S.C. §119
SE	9503343-7	27 September 1995	X Yes __ No
			__ Yes __ No
			__ Yes __ No
			__ Yes __ No
			__ Yes __ No

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below.

(Application Number) (Filing Date)

(Application Number) (Filing Date)

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY (CONTINUED)
(Includes Reference to Provisional and PCT International Applications)

ATTORNEY'S DOCKET NO.
027555-959

I hereby claim the benefit under Title 35, United States Code, §120 of any United States applications(s) or PCT international application(s) designating the United States of America that is/are listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose to the Office all information known to me to be material to the patentability as defined in Title 37, Code of Federal Regulations §1.56, which became available between the filing date of the prior application(s) and the national or PCT international filing date of this application:

PRIOR U.S. APPLICATIONS OR PCT INTERNATIONAL APPLICATIONS DESIGNATING THE U.S. FOR BENEFIT UNDER 35 U.S.C. 120:

U.S. APPLICATIONS		STATUS *(check one)*		
U.S. APPLICATION NUMBER	U.S. FILING DATE	PATENTED	PENDING	ABANDONED

PCT APPLICATIONS DESIGNATING THE U.S.

PCT APPLICATION NO.	PCT FILING DATE	U.S. APPLICATION NUMBERS ASSIGNED (If any)			
PCT/SE96/01156	18 September 1996			X	

I hereby appoint the following attorneys and agent(s) to prosecute said application and to transact all business in the Patent and Trademark Office connected therewith and to file, prosecute and to transact all business in connection with international applications directed to said invention:

William L. Mathis	17,337	Ralph L. Freeland, Jr.	16,110	William C. Rowland	30,888
Peter H. Smolka	15,913	Robert G. Mukai	28,531	T. Gene Dillahunty	25,423
Robert S. Swecker	19,885	George A. Hovanec, Jr.	28,223	Anthony W. Shaw	30,104
Platon N. Mandros	22,124	James A. LaBarre	28,632	Patrick C. Keane	32,858
Benton S. Duffett, Jr.	22,030	E. Joseph Gess	28,510	Bruce J. Boggs, Jr.	32,344
Joseph R. Magnone	24,239	R. Danny Huntington	27,903	William H. Benz	25,952
Norman H. Stepno	22,716	Eric H. Weisblatt	30,505	Peter K. Skiff	31,917
Ronald L. Grudziecki	24,970	James W. Peterson	26,057	Richard J. McGrath	29,195
Frederick G. Michaud, Jr.	26,003	Teresa Stanek Rea	30,427	Matthew L. Schneider	32,814
Alan E. Kopecki	25,813	Robert E. Krebs	25,885	Michael G. Savage	32,596
Regis E. Slutter	26,999	Robert M. Schulman	31,196	Gerald F. Swiss	30,113
Samuel C. Miller, III	27,360				

and: Steven M. du Bois, Registration No. 35,023

Address all correspondence to: **Ronald L. Grudziecki**
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, Virginia 22313-1404

Address all telephone calls to: Ronald L. Grudziecki at (703) 836-6620.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

(1/96)

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY (CONTINUED) (Includes Reference to Provisional and PCT International Applications)		ATTORNEY'S DOCKET NO. 027555-959
FULL NAME OF SOLE OR FIRST INVENTOR Roland BODIN	SIGNATURE Roland Bodin	DATE 270123
RESIDENCE Gribbyvägen 55, 163-59 Spånga, Sweden		CITIZENSHIP Swedish
POST OFFICE ADDRESS Gribbyvägen 55, 163-59 Spånga, Sweden		
FULL NAME OF SECOND JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE		CITIZENSHIP
POST OFFICE ADDRESS		
FULL NAME OF THIRD JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE		CITIZENSHIP
POST OFFICE ADDRESS		
FULL NAME OF FOURTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE		CITIZENSHIP
POST OFFICE ADDRESS		
FULL NAME OF FIFTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE		CITIZENSHIP
POST OFFICE ADDRESS		
FULL NAME OF SIXTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE		CITIZENSHIP
POST OFFICE ADDRESS		
FULL NAME OF SEVENTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE		CITIZENSHIP
POST OFFICE ADDRESS		
FULL NAME OF EIGHTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE		CITIZENSHIP
POST OFFICE ADDRESS		
FULL NAME OF NINTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE		CITIZENSHIP
POST OFFICE ADDRESS		